



Emergency Management and Response Information Sharing and Analysis Center (EMR-ISAC)

INFOGRAM 15-08

April 17, 2008

NOTE: This INFOGRAM will be distributed weekly to provide members of the Emergency Services Sector with information concerning the protection of their critical infrastructures. For further information, contact the Emergency Management and Response- Information Sharing and Analysis Center (EMR-ISAC) at (301) 447-1325 or by e-mail at emr-isac@dhs.gov.

Terrorism: Urban versus Rural America

A recent terrorism study funded by the Department of Homeland Security ranked 132 American cities according to their vulnerability to a terrorist attack. A lead researcher in the four-year analysis clarified that the resultant report focuses on how well a city could withstand an attack based on three factors: socioeconomics, infrastructure, and geophysical hazards. The Emergency Management and Response—Information Sharing and Analysis Center (EMR-ISAC) verified the information does not address whether a city would make an attractive target, but only its vulnerability if the city was attacked. For example, terrorists are known to gauge the success of their attacks based on the amount of casualties, destruction, disruption, and fear caused by their actions. Therefore, an attack on an unsuspecting and unprepared city might produce these results. An abstract of this study can be seen at: <http://www.blackwell-synergy.com/doi/abs/10.1111/j.1539-6924.2007.00977.x>.

Since many cities considered high profile and attractive to terrorists are currently attempting to reduce or eliminate their vulnerabilities, it is highly probable that our adversaries will turn their attention away from urban environments to much lower profile rural areas of the United States. In fact, the EMR-ISAC has reviewed other studies by homeland security professionals who confirm the urgency for the protection of the “vitally and strategically important” critical infrastructures found throughout the rural regions of America. Much of the nation’s food supply, water sources, and essential industries (e.g., power plants, water treatment facilities, dams) are located in rural areas. Consequently, some security specialists claim that “rural communities bring with them unique ‘all-hazards’ protection challenges that are far different than their urban counterparts.”

In its report, “Preparing for Public Health Emergencies: Meeting the Challenge in Rural America,” the Harvard Center for Public Health Preparedness recommended action by policy makers at all levels of government as well as by the leaders of the emergency and public health services. Specifically, the report advocated the following activities for America’s rural areas:

- Apply adequate preparations to protect citizens from man-made and natural disasters.
- Strengthen the emergency and public health systems.
- Provide the financial and human resources to achieve acceptable readiness.
- Ensure emergency preparedness is accomplished in a cost-effective manner.

This 36-page (2.46MB) document can be viewed at http://www.prepare.pitt.edu/pdf/crhp_agenda.pdf. The Rural Assistance Center is another helpful link for rural communities: <http://www.raonline.org>.

Cyber Security Challenges for ESS Organizations

In a speech delivered last week, Homeland Security Secretary Michael Chertoff discussed the current cyber security challenges facing the United States and its critical infrastructure sectors. He divided the challenges into three broad categories: criminals attempting to steal or extort money, the theft of information or espionage, and attacks to disrupt or destroy systems. Secretary Chertoff emphasized that “these are serious problems for our nation that will grow more serious as time passes.” He lamented that “we have to recognize we are operating in a domain in which the power of government is insufficient to address the full nature of the threat.”

To combat this growing problem, the Department of Homeland Security (DHS) established the National Cyber Security Division to manage cyber threats against the government. Additionally, DHS created the U.S. Computer Emergency Readiness Team (US-CERT) to provide 24-hour watch and warning for the nation's Internet infrastructure. Secretary Chertoff added that organizations and their employees of the public and private sectors can prevent security breaches: by getting more serious and dedicated about internal security; by ensuring no one brings viruses, Trojan Horses, and worms into their systems and networks; and by enforcing cyber privacy.

The Emergency Management and Response—Information Sharing and Analysis Center (EMR-ISAC) also confirms that unprecedented interdependencies continue to create vulnerabilities with potential disruptions to Emergency Services Sector (ESS) capabilities such as computer-aided dispatching. This is a dangerous threat to emergency departments and agencies because computers and cyber networks have become an integral part of the ESS critical infrastructures that cannot be interrupted or destroyed without jeopardizing response operations.

Assistant Secretary for Cyber Security Greg Garcia recently explained, "We all depend on shared critical infrastructures and systems to maintain our national security." He called on every organization using networked technology to accept responsibility for securing their part of cyberspace by taking cyber risks seriously, ensuring that any potential cyber incidents, threats, or attacks are reported to the US-CERT at (888) 282-0870, and by using the safeguards available at the federal web site, "OnGuardOnline" (<http://onguardonline.gov/index.html>).

Strategies to Protect ESS Assets

Recessionary economies can adversely affect Emergency Services Sector (ESS) critical assets through funding losses that necessitate actions such as reductions in force. To help sector leaders prepare for and prevent proposed cuts in internal infrastructures (i.e., personnel, physical assets, and communication/cyber systems), the International Association of Fire Fighters (IAFF) revised its "Surviving an Economic Crisis" guide.

The guide advises ESS organizations to understand how their respective local governments operate to gain insight into how to evaluate funding threats. It urges emergency organizations to identify resources, develop a strategy, and plan to prevent or mitigate adverse actions on organizational budgets and individual members' benefits. Explaining the process begins with the hypothetical example of a city notifying the ESS that it is seeking a significant personnel reduction in force. To contend with the threat of funding losses, the guide recommends the following actions, summarized by the Emergency Management and Response—Information Sharing and Analysis Center (EMR-ISAC):

- Pinpoint and catalogue internal and external resources (e.g., members, legal counsel, advocates, coalition partners, financial analysis, community activists) that departments have or may need.
- Understand the jurisdiction's system and the public laws and procedures that govern it. What key provisions would govern downsizing initiatives?
- Identify the problem components: degree of urgency and severity, long-term versus short-term effects, evidence of a history of problem/issue, and all possible outcomes associated with the problem.
- Develop a solution strategy that specifies desired outcomes and identifies relationships and partnerships, and create a communications plan and core message to use for members, the community, and on the political front.
- Delineate the elements of an action plan: choose goals, gather information, identify needs, determine resources, list key implementation steps, implement plan, and adjust plan as needed.

To enable ESS readiness to respond to potential downsizing areas (response system, personnel, collective bargaining agreements, pension, health benefits, compensation, and leave), the guide lays out recommended preparation, strategies, key tactics, resources, and process. "Surviving an Economic Crisis" (26 pp., 2.51 MB) can be downloaded at <http://www.iaff.org/Comm/PDFs/EconomicCrisis.pdf>.

Center for Domestic Preparedness

The Department of Homeland Security (DHS) offers fully funded all-hazards training to help state, local, and tribal Emergency Services Sector (ESS) personnel manage threats to their critical infrastructures at its Center for Domestic Preparedness (CDP) in Anniston, Alabama.

Responders from all ESS disciplines in the 50 states, District of Columbia, and all U.S. territories have participated in the CDP's interdisciplinary resident and nonresident preparedness, deterrence, and response courses since it opened in 1998. Its Chemical, Ordnance, Biological and Radiological Training Facility (COBRATF) is the only training program in the nation that features advanced, hands-on civilian training exercises "in a true toxic environment using chemical agents." Last year, the Noble Training Facility (NTF), a nearby former army hospital, was integrated into the CDP. It is now the only hospital facility in the country exclusively for training hospital and health care professionals in disaster preparedness and response.

Resident courses are offered for emergency management, law enforcement, emergency medical services, fire service, public works, public safety communications, hazmat, health care (non-EMS), public health, and government administrative personnel. The CDC pays for transportation, lodging, and meals. Nonresident training is presented at no charge in responders' home jurisdictions by CDP's Mobile Training Teams. Local sponsors are responsible for reserving a training site and making necessary logistical arrangements. A total of 23 nonresident courses (awareness, performance defensive, health care, and management and planning) can be scheduled, most of which require a minimum of 50 students.

The Emergency Management and Response—Information Sharing and Analysis Center (EMR-ISAC) suggests responders consider the CDP's fully funded training opportunities. Course descriptions and schedules, application forms for resident courses, how-to-schedule nonresident course information, state points of contact, regional coordinator contacts, and testimonials from former students are available by visiting <https://cdp.dhs.gov> and clicking on "Continue with Limited Functionality."

FAIR USE NOTICE

This INFOGRAM may contain copyrighted material that was not specifically authorized by the copyright owner. EMR-ISAC personnel believe this constitutes "fair use" of copyrighted material as provided for in section 107 of the U.S. Copyright Law. If you wish to use copyrighted material contained within this document for your own purposes that go beyond "fair use," you must obtain permission from the copyright owner.

The National Infrastructure Coordinating Center (NICC) within the Department of Homeland Security (DHS) Office of Infrastructure Protection is the central point for notifications regarding infrastructure threats, disruptions, intrusions, and suspicious activities. Emergency Services Sector personnel are requested to report any incidents or attacks involving their infrastructures using at least the first and second points of contact seen below:

- 1) NICC - Voice: 202-282-9201, Fax: 703-487-3570, E-Mail: nicc@dhs.gov
- 2) Your local FBI office - Web: <http://www.fbi.gov/contact/fo/fo.htm>
- 3) EMR-ISAC - Voice: 301-447-1325, E-Mail: emr-isac@dhs.gov, fax: 301-447- 1034,
Web: www.usfa.dhs.gov/subjects/emr-isac, Mail: J-247, 16825 South Seton Avenue,
Emmitsburg, MD 21727